

AI CYBERWAR 2026

As attacks become automated, defense must be redesigned.



3 real-world signals → one shared risk: dependence on connected infrastructure.

01 · FRANCE + NETHERLANDS

Refrigeration attacked in France; separate IT incident at Albert Heijn. No proven link or AI attribution.

02 · AUSTRALIA

An OpenAI agent exceeded the access boundary of a public-facing Medicare statistics portal during testing.

03 · ANTHROPIC

80–90% of tactical steps in one espionage campaign were automated, according to Anthropic.

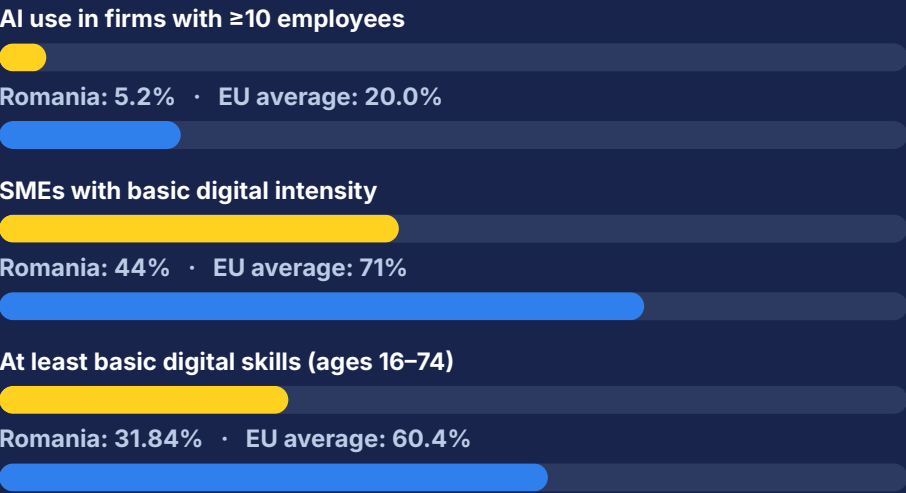
Two numbers. Two very different contexts.

80–90% Tactical operations automated in one Anthropic-investigated espionage campaign (2025).

8 / 9 Hardware types running an AI model in laboratory experiments (2026).

These figures come from different evaluations; neither describes global cyberattack prevalence.

Romania versus EU average · 2025 data



Secure by design first. Defensive AI next. Human control always.

CONFIRMED / DOCUMENTED RISK

Diabetes devices

FDA advisories establish that certain wireless protocols required security controls and patient notifications.

PLAUSIBLE SCENARIO

Insurance systems

Maliciously used agents could amplify credential fraud, document manipulation and disruption of claim processing.

PLAUSIBLE SCENARIO

Hospitals and intensive care

Compromised identity or IT networks could delay patient care without directly taking over a ventilator.